自治体クラウドの情報セキュリティ対策等に関する調査研究

報告書　概要版

2013年5月

総務省

目次

本調査研究の概要

【本調査の目的】

下記の2テーマを中心に、今後自治体クラウドに取り組もうとする自治体が留意すべき事項について調査研究を行い、その成果を普及することにより、自治体クラウドの一層の推進に資することを目的とする。

1 自治体クラウドの情報セキュリティ対策

- 国内外におけるセキュリティ事案の動向
- クラウド事業者におけるセキュリティ対策の評価
- 責任分界の在り方
- ネットワーク障害時に備えた対策
- クラウド環境におけるセキュリティポリシー

2 番号制度を踏まえた自治体クラウドの推進のあり方

- 番号制度の概要
- 中間サーバの共同利用
- 想定される共同利用の形態（ネットワーク構成のあり方等）
- 導入スケジュール（想定）
- 番号制度の導入に係るヒアリング結果について

1. 自治体クラウドの取り組み状況

総務省、財団法人地方自治情報センター（LASDEC）等を中心に、平成21年度から実証実験などを行い、先進的な自治体については、実システムとして運用が開始されている。これまでの経験などを踏まえて、自治体クラウドには下記のような効果や課題があることが認識されている。

自治体クラウド導入による効果

- 情報システムに係るコスト削減
- 情報システムの管理・運用業務軽減
- 業務プロセス標準化による業務効率化
- 情報セキュリティの確保
- 住民サービスの向上
- 災害への対応強化

自治体クラウド導入にあたっての課題

- カスタマイズの制約
- 相互運用性の確保
- 情報セキュリティに係る技術的対策
- 情報セキュリティに係る法的留意点

（出典：LASDEC「地方公共団体におけるクラウド導入の取組み」を基に作成
https://www.lasdec.or.jp/cms/9,26589,21.html）

2. 自治体クラウドの情報セキュリティ対策 （1）

（2－1） 国内外におけるセキュリティ事案の動向

近年の国内外におけるサイバー攻撃等のセキュリティ事案として特に注目すべき内容は以下の通り。

1）標的型攻撃

- 標的型攻撃とは、組織内の従業員・職員等を標的として巧妙に作られたメールを送り付けてシステムにウィルスを感染させ、外部からの侵入口を作り、情報搾取などを行うものである。IPAの2012年版10大脅威では1位となっており、新たに顕在化した脅威として挙げられている。
- 標的型攻撃はAPT（Advanced Persistent Threat：先進的で執拗な脅威）とも呼ばれており、従業員の情報を電話などのオフラインで入手するなど、ソーシャルエンジニアリングの手法を組み合わせることもあり、手口が年々巧妙化している。

2）不正アクセス

- 大手企業や官庁を攻撃対象にした悪意を持つ集団による攻撃が増えている。不正アクセス自体は古くから行われている攻撃手法だが、ソフトウェアの脆弱性が絶え間なく発見されるため、不正アクセスの脅威は継続していると言える。IPAの10大脅威でも、ウェブサイトを狙った攻撃は2007年から毎年取り上げられている。
- 近年では、不正アクセスが組織化しており、悪意を持つものと不正アクセスを行うものが分業化しているため、不正アクセスの対象になりやすい大手企業や官庁の脅威は増している。

3）制御システムに対する攻撃

- 従来は外部ネットワークとの接続を行っていないために、サイバー攻撃等とは無縁と考えられてきた制御システムにおけるセキュリティインシデントが増加している。NISCの第2次行動計画においても制御システムに対する注意喚起が行われており、IPAにおいても制御システムに対するセキュリティ対策に関する取り組みが始まっている。
- とりわけ、2009年にイランの核施設における遠心分離器の破壊を狙ったStuxnet（スタックスネット）と呼ばれるマルウェアは、標的型攻撃を制御システムに対して行った代表的な事例として注目されており、同様の手法で多くの制御システムが攻撃できる可能性を示した。

2. 自治体クラウドの情報セキュリティ対策 （2）

（2－2） クラウド事業者におけるセキュリティ対策の評価（1）

自治体クラウドとして留意すべき情報セキュリティ対策項目について、自治体クラウドに先進的に取り組んでいる5団体にヒアリング調査を行った結果、特に留意している項目を以下に示す。

情報セキュリティ項目	ヒアリング対象団体				
	A	B	C	D	E
共同利用時の料金負担の公平性		○		○	
不明瞭なSLA			○		
ノンカスタマイズの場合の業務改革コスト	○			○	
ベンダロックイン		○			○
セキュリティモデル、品質モデルのカスタマイズ		○	○	○	
既存システムとのデータ連係					○
アクセス権限の管理（クラウド事業者側を含む）					○
アプリケーションの応答速度	○				○
データ保管場所と法制度		○	○	○	
ソフトウェアライセンスの移行					

記号：○=留意している

2. 自治体クラウドの情報セキュリティ対策 （3）

（2－2） クラウド事業者におけるセキュリティ対策の評価（2）

クラウド事業者側のセキュリティ対策と、自治体クラウドとして留意すべき情報セキュリティ対策項目を比較し、クラウド事業者を評価を行う仕組みを検討した。検討結果の案を以下に示す。

セキュリティリスク	クラウド事業者評価の仕組み（案）
共同利用時の料金負担の公平性	● 自治体の規模の違いによる料金負担が適切かどうかを確認する。 ● 小規模な自治体に不要な機能により、料金が高くなっていないことの確認が必要である。
不明瞭なSLA	● SLAの内容を確認する。 ● 具体的なSLA項目については「（2-3） 責任分界の在り方」に示す。
ノンカスタマイズの場合の業務改革コスト	● 従来システムからクラウドシステムへの移行時において、エンドユーザへの説明会等の開催、エンドユーザにとってわかりやすいマニュアル類の提供などを確認する。
ベンダロックイン	● ベンダロックインについては、特にデータ移行の際に注意を要する。中間フォーマットなどの標準形式でデータをエクスポートできる機能や、それらのエクスポートデータ作成のコストなどの確認が必要である。
セキュリティモデル、品質モデルのカスタマイズ	● セキュリティや品質に係るカスタマイズの柔軟性が確保されていることを確認する。クラウドとして標準的に提供されるセキュリティの水準に加えて、セキュリティを強化するためのオプションが選択可能かどうかを確認する。
既存システムとのデータ連携	● 自治体クラウドへの移行の過渡期において、庁内の既存システムとのデータ連携が可能かどうか確認する。
アクセス権限の管理（クラウド事業者側を含む）	● クラウドの管理者に対する役割分担と責任分界が定められていることを確認する。 ● 団体毎の管理者や、複数団体を束ねた管理者など、クラウド共同利用の形態に即した管理者権限、ユーザ権限が付与可能か確認する。
アプリケーションの応答速度	● アプリケーション応答速度に関してSLAで定めているか、また定めたとおりのパフォーマンスが出ていることを利用者側で確認する仕組みがあるかを確認する。
データ保管場所と法制度	● データセンター、バックアップの管理について確認をする。特にバックアップデータの取得頻度や保管先、個人情報等の機微情報に対する特別な取扱いの有無について確認をする。

2. 自治体クラウドの情報セキュリティ対策 （4）

（2－3） 責任分界の在り方（1）

自治体クラウドにおいて必要とされるSLA項目について、自治体クラウドに先進的に取り組んでいる5団体にヒアリング調査を行った結果を以下に示す。

SLA項目	ヒアリング対象団体				
	A	B	C	D	E
サービス時間（24時間365日、など）	○	○	○	○	○
サービス稼働率（99.9%、など）	○	○	○	○	○
ディザスタリカバリ方法（遠隔地へのデータバックアップ、など）	○	○			
障害発生時等に提供されるバックアップデータ形式（標準フォーマット、など）				○	
平均復旧時間（1時間以内、など）	○				○
サービス提供状況の確認方法（ホームページ上で公開、など）	○	○	○	○	
カスタマイズ性（利用者側でのカスタマイズ可能な項目、など）					
同時接続利用者数（同時50ユーザ、など）					
データバックアップの方法	○	○	○	○	
バックアップデータの保管期間	○	○			

記号：○=規定している

2. 自治体クラウドの情報セキュリティ対策 （5）

（2－3） 責任分界の在り方（2）

自治体クラウドで必要とされるSLA項目について、ヒアリング対象団体の取り組みなどを参考として、求めるべきグレードの案を検討した。

SLA項目	求めるべきグレード（案）
サービス時間	● 市民向けサービスについては24時間365日（サービス停止時間は別途定める） ● 職員向けサービスについては、開庁日時を基準に個別の事情に合わせて定める。 ● 夜間バッチ処理に必要なサービス時間も別途定める。
サービス稼働率	● 99%～99.5%程度を基本とする。
ディザスタリカバリ方法	● 広域災害を想定した遠隔地へのバックアップが行われていること。 ● 遠隔地のバックアップデータを用いた緊急対応の方法が定められていること。
障害発生時等に提供されるバックアップデータ形式	● EUC（エンドユーザコンピューティング）で利用可能なデータ形式でデータが提供されること。
平均復旧時間	● 3時間程度を基本とする。
サービス提供状況の確認方法	● オンラインでリアルタイムにサービス稼働状況が確認できること。 ● 障害発生時には、自治体の管理者宛に電話やメールなど複数手段で自動的に連絡すること。
カスタマイズ性	● 簡易な帳票の変更が利用者側で可能なこと。 ● EUCで利用可能なデータ形式で出力可能なこと。
同時接続利用者数	● 平常時に利用可能な同時接続利用者数を定めること。 ● 特別な理由で同時接続利用者数が増えた場合に、一時的に増やす手段や手続きを定めること。
データバックアップの方法	● バックアップの頻度、方法（フル、差分など）、保管媒体、バックアップデータ形式を定めること。
バックアップデータの保管期間	● バックアップの保管期間、保管する世代数、廃棄時の方法を定めること。

2. 自治体クラウドの情報セキュリティ対策 （6）

（2－4） ネットワーク障害時に備えた対策（1）

ネットワーク障害パターンとして、平常時の機器故障や、通信事業者やクラウド事業者側の障害、大規模災害時の広域障害などを類型化し、それぞれの状況を整理した。

ネットワーク障害のパターン	通信事業者			クラウド事業者			自治体庁舎	
	基幹網	局舎	アクセス回線	ハードウェア	基盤ソフトウェア	アプリケーション	通信機器	端末
(1)単独の通信障害			×					
(2)大規模通信障害	×							
(3)クラウドのハードウェア障害				×				
(4)クラウドのソフトウェア障害					×	×		
(5)自治体の通信機器障害							×	
(6)自治体の端末障害								×
(7)局所的な停電							×	×
(8)大規模災害時の広域障害（停電なし）	×	×	×					
(9)大規模災害時の広域障害（停電あり）	×	×	×				×	×

記号：×=障害発生

2. 自治体クラウドの情報セキュリティ対策 （7）

（2－4） ネットワーク障害時に備えた対策（2）

ネットワーク障害発生時の対策について、前項のネットワーク障害パターン別に検討した。ネットワーク障害パターンと主な対策の対応を下表に示す。

ネットワーク障害のパターン	主な対策					
	アクセス回線を多重化	自庁社内機器の代替機を確保	自庁舎内にバックアップサーバを設置	自庁舎内にデータバックアップを確保	自庁舎に非常用発電装置等を備える	クラウド側の冗長化をSLA等で規定
(1)単独の通信障害	○		○			
(2)大規模通信障害			○	○		
(3)クラウドのハードウェア障害			○			○
(4)クラウドのソフトウェア障害			○			○
(5)自治体の通信機器障害	○	○				
(6)自治体の端末障害		○				
(7)局所的な停電	○				○	
(8)大規模災害時の広域障害（停電なし）			○			
(9)大規模災害時の広域障害（停電あり）			○		○	

記号：○=障害のパターンに関係する対策

2. 自治体クラウドの情報セキュリティ対策 （8）

（2－5） クラウド環境におけるセキュリティポリシー

自治体クラウドにおける個人情報取扱いに関する課題を含めて、従来のセキュリティポリシーを自治体クラウド向けに見直す場合の、検討のポイントなどをヒアリング結果からまとめた。

見直しの検討ポイント	ヒアリング結果のまとめ
セキュリティポリシーの共同化と適用の範囲	• 複数団体で共同化を進める場合、クラウド環境のデータセンターやネットワークまでを共通化するセキュリティポリシー適用の範囲とし、各団体内のネットワークについては共同化の対象外とするケースがある。このように切り分けることで、比較的容易にセキュリティポリシーの共同化が可能である。 • クラウドによる共同化で、各団体でばらばらであった個人情報の取扱いが共通化される。この際に情報審議会にかけるかどうかは、団体毎の条例の解釈の違いに依存する。
クラウド環境に適応したネットワーク構成	• ネットワーク構成の変更に伴い、セキュリティポリシー見直しの要否も検討が必要となる。
クラウド化対象の違いによる見直しの要否	• 公共施設、電子申請などでクラウド化を実施した際にはセキュリティポリシーは変えなかった。しかし、住民情報系のクラウド化に際しては、セキュリティポリシーを見直す必要があると感じている。 • 従来のセキュリティポリシーの程度によっても要否は異なる。クラウドに変更する以前から基本的なID・パスワードの管理、個人情報の管理、メディアの管理などを厳格に定めていた団体では、クラウド化によっても変更せずに対応できるケースもある。
クラウド事業者の選定基準	• 個人情報を扱う場合には、適切なクラウド事業者の選定基準が必要である。 • サービス要件定義書において、クラウド事業者に対して、ISO27001/ISMSやプライバシーマークの取得を求める団体もある。
クラウド化に特化したセキュリティポリシー見直し項目	• クラウド化を前提としたセキュリティポリシーにおいては、従来システムにおけるセキュリティポリシーに加えて、データの保管場所、暗号化、バックアップ、通信の暗号化、強固なユーザ認証、アクセス制限、セキュアなアプリケーションなども検討する必要がある。

３．番号制度を踏まえた自治体クラウドの推進のあり方 （１）

（３－１） 番号制度の概要

番号制度とは、社会保障の充実・安定化と、そのための安定財源確保と財政健全化の同時達成を目指す社会保障と税の一体改革を推進するため必要な基盤として導入が検討されている制度であり、政府・与党社会保障改革本部により検討が進められてきた。「社会保障・税番号大綱（平成23年6月30日、政府・与党社会保障改革本部決定）」では、番号制度により実現できること及び必要な仕組みについて、以下のように記載されている。

（1）よりきめ細やかな社会保障給付の実現

（2）所得把握の精度の向上等の実現

（3）災害時における活用

（4）自己の情報や必要なお知らせ等の情報を自宅のパソコン等から入手できる

（5）事務・手続の簡素化、負担軽減

（6）医療・介護等のサービスの質の向上等

上記の検討に基づき、平成25年3月1日、番号制度を実現するための法律案として「行政手続における特定の個人を識別するための番号の利用等に関する法律案（以下、「番号法案」という。）」が第183回通常国会に提出された。

番号法案別表第一では、個人番号を利用できる者及び事務の一覧が示されている。また、番号法案別表第二では、特定個人情報の情報照会者及び事務に対して、情報照会できる特定個人情報及びその情報提供者の一覧が示されている。

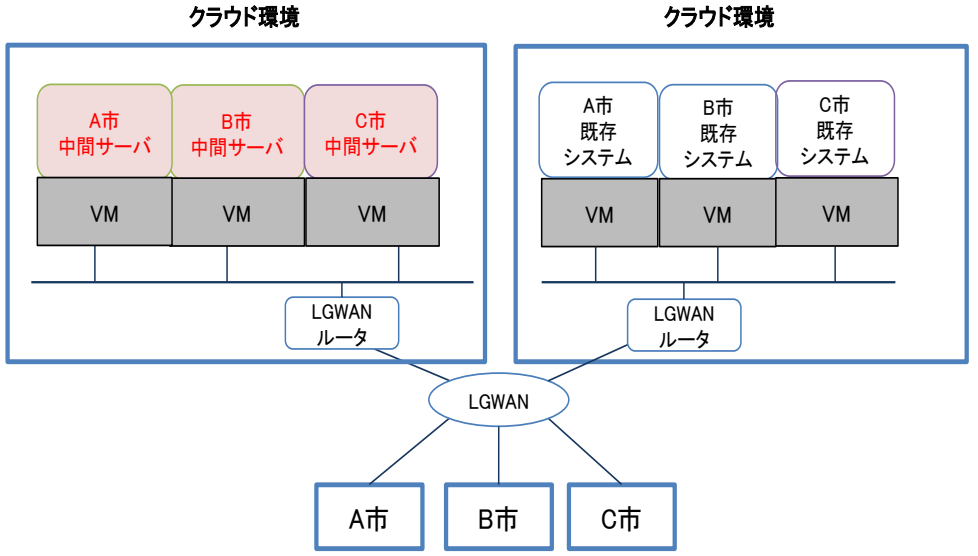
3. 番号制度を踏まえた自治体クラウドの推進のあり方 （2）

（3－2） 中間サーバの共同利用

- 地方公共団体においては、「中間サーバ」を導入することが考えられる。
- 自治体クラウドを活用して中間サーバの共同利用を行う場合の主な効果と課題、及び中間サーバの共同利用イメージについて、以下のように検討した。

表　中間サーバ共同利用の主な効果と課題

主な効果	概要	主な課題	概要
コスト削減	中間サーバの機能は共通性が高く、カスタマイズの必要性は比較的少ないと考えられるため、コスト削減の余地は大きい。	カスタマイズの制約	少なからず発生が想定されるカスタマイズの範囲や、共同利用団体間での仕様の差異を最小化するための調整を行う必要がある。
情報セキュリティの確保	データセンター等に設置されるため、一定の情報セキュリティレベルが確保される。	費用按分の方法	トラフィック量が各団体の人口規模に加え、情報照会、情報提供の量にも依存するため、望ましい按分方法を検討、調整する必要がある。



VM:Virtual Machine（仮想マシン）の略。

図　中間サーバ共同利用のイメージ

3. 番号制度を踏まえた自治体クラウドの推進のあり方 （3）

（3－3） 想定される共同利用の形態

- 中間サーバで想定される共同利用の形態について、既存システムの共同利用の形態と比較した場合に考えられる特徴について、下表の通り整理した。
- また、ネットワーク構成のあり方については、以下のような観点から検討を行う必要があると考え、例示として、基幹系LANと情報系LANが分かれている場合のネットワーク構成例を示した。

表　共同利用における既存システムと中間サーバの特徴

観点	既存システムの特徴	中間サーバの特徴
集約範囲	業務システムの要件が団体毎に異なるため、SaaSの導入は調整を要する。	ソフトウェア仕様の共通性が高いため、SaaSの導入が容易と考えられる。
対象団体	地域性や業務内容に違いがあるため、無条件な対象団体の増加は調整を要する。	制度同時期、全団体の一斉稼働が求められる場合、対象団体を広げることが比較的容易と考えられる。

表　ネットワーク構成の検討観点

観点	概要
責任分界点の明確化	既存システムや情報提供ネットワークシステムとの責任分界点が明確となるような構成とする必要がある。
セキュリティの確保	中間サーバは、情報提供ネットワークシステムを介して他の情報保有機関とやり取りを行うため、十分なセキュリティを確保できるようなネットワーク構成とする必要がある（ファイアウォールの設置など）。
自庁内ネットワーク	中間サーバを情報系LANに接続するか、中間サーバと情報系LANとの間にFWを設置するか等の検討が必要となる。

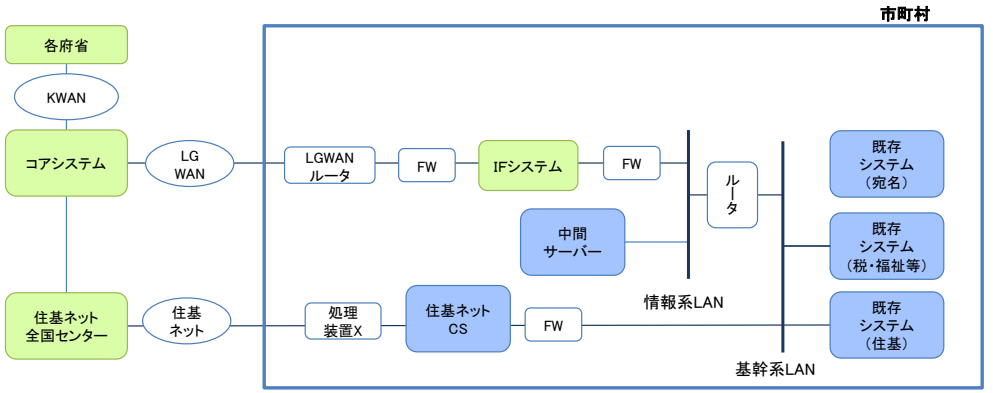


図　基幹系LANと情報系LANが分かれている場合の構成例
（中間サーバを情報系LANに直接接続するケース）

3. 番号制度を踏まえた自治体クラウドの推進のあり方 （4）

（3－4） 導入スケジュール（想定）

- 導入スケジュールについては、平成24年度における番号法案の提出時に示されたロードマップ（案）から、約1年程度後ろ倒しで進められることが予想されている。
- 想定される導入スケジュールについては、以下のとおりとした。

表　想定される導入スケジュール

時期（想定）	マイルストーン（想定）
2015(H27)年　秋頃	• 住民へのマイナンバーの通知（通知カードの交付・送付）開始
2016(H28)年1月	• 個人番号カードの交付開始（通知カードと引換）
2017(H29)年1月	• 情報提供ネットワークシステムの運用開始 • 国の機関間における情報連携の開始 • 情報提供等記録開示システムの稼働
2017(H29)年7月	• 地方公共団体を含めた情報連携の開始

3. 番号制度を踏まえた自治体クラウドの推進のあり方 （5）

（3－5） 番号制度の導入に係るヒアリング結果について

- 番号制度の導入に係るヒアリング結果の概要について、以下に示す。

表　番号制度の導入に係るヒアリング結果（概要） 1／2

調査項目	概要
業務システムの共同化、クラウド化の状況について	● 番号法案別表第2で示された事務のうち、基幹系業務については、概ねクラウドによる共同利用を実施している（又は実施予定である）団体が多い。 ● 一方、福祉系の事務については、共同利用やシステム化が行われていない場合も多い。その場合は、別途システム化を行うか、専用端末からの入力が必要となると考えられる。
検討・推進体制について	● 自治体クラウドの取り組みを実施している（又は実施予定である）ため、それとは別に番号制度の導入のために、別途推進体制を設けたというヒアリング団体は存在しなかった。今後は、既存システムの自治体クラウドに係る協議会や定例会等において、番号制度の導入についても検討していく意向の団体が多い。 ● 番号制度に関する情報は、内閣官房が実施した説明会（シンポジウム）への参加や、ベンダからの提案等を通じて取得している団体が多かった。
調達について	● 自治体クラウドを実施している（又は実施を予定している）ため、従来の契約（又は予定している契約）と同等の方式で調達する方針であるとのことである。 ● 新規に調達を行うのではなく、制度改正による対応の一環として、（費用の有無は別として）既存契約内での対応を想定している団体が多い。
中間サーバのクラウド利用について	● 全てのヒアリング団体について、既存システムと同様に、中間サーバについてもクラウドによる共同利用を行う意向であった。 ● クラウドの利用形態（SaaS、PaaS、IaaSなど）についても、現在実施中の自治体クラウドの利用形態（又は予定している形態）を踏襲する方針の団体が多いが、複数のパターンを想定している団体も存在する。

3. 番号制度を踏まえた自治体クラウドの推進のあり方 （6）

表　番号制度の導入に係るヒアリング結果（概要） 2／2

調査項目		概要
費用負担、参加団体について		● 費用負担についても、現在実施中の自治体クラウドの利用形態（又は予定している形態）を踏襲する方針の団体が多いが、具体的な按分方法等まで検討していない団体もあった。 ● 参加団体については、番号制度を機に、参加団体を増加させる意向を持つヒアリング団体も存在したため、番号制度の導入が、自治体クラウド推進のトリガーとなり得ると考えられる。
法制度・規約類の対応について		● 自治体クラウド実施団体では、すでに外部接続に関する条例等の対応は完了しているため番号制度の導入に当たり、新たな対応は予定していない（必要がない）。ただし、新規に取り組む団体では、新たに外部システム（情報提供ネットワークシステム等）との接続が必要になるため、外部接続に伴うセキュリティポリシーの修正を見込んでいるヒアリング団体が存在した。 ● 個人情報保護条例については、除外規定として、「法令に定めのあるとき」という条項を設けているため、特段の対応を講じる必要はないとのことであった。 ● 情報照会、情報提供に当たっては、文書管理規程等で課内決裁等が必要になりうる団体が存在する。そのため、番号制度の導入に当たって文書管理規程を変更する、情報照会、情報提供に当たって電子決裁機能を具備する等の対応が必要になる可能性がある。
その他のテーマ	同一庁内の連携	● 実態として同一庁内に存在する複数の情報保有機関（「市区町村」と「市区町村教育委員会」等）について、番号法案では、自庁内で連携するためには条例を策定する必要があるとされている（番号法案第十九条第九号）。しかしながら、現行のシステムで実現できていることを引き続き行うために条例を制定するのは現実的でない。
	画面上での情報確認について	● 所得証明書などの町村間の情報照会は、紙媒体で実施している。原課としては、番号制度対応により、これまで紙で確認していたものを画面で確認することになるため、切り替えのハードルは高いと思われる。また、データの真正性をどう担保するかも課題となる。
	既存システムの宛名統一	● 番号制度の導入に当たっては、個人番号又は符号と紐付ける既存システム側の宛名番号について、団体内で統一されていることが望ましい可能性がある。しかしながら、宛名の統一がなされていない団体も存在し、それらの団体については、予め宛名を統一する必要があり、団体の負担となりうる。

4. まとめ

1 自治体クラウドの情報セキュリティ対策

- 自治体クラウドの情報セキュリティ対策として、クラウド事業者によるセキュリティ対策の評価、SLA項目の設定による責任分界の在り方、ネットワーク障害に備えた対策、セキュリティポリシー見直し等について検討を行った。
- 自治体クラウドに先進的に取り組んでいる自治体では、クラウドシステム利用開始からちょうど1年程度経過している。この1年でクラウドのセキュリティ対策については多くの知見が蓄積されてきており、これらの知見は今後自治体クラウドに取り組む多くの自治体に有効と言える。

2 番号制度を踏まえた自治体クラウドの推進のあり方

- 中間サーバの導入に当たっては、既に既存システムの自治体クラウドを推進している団体はもちろんのこと、現時点で自治体クラウドに取り組んでいない団体に対しても、自治体クラウドの効果を訴求できるものと考える。加えて、中間サーバの導入をきっかけとして、既存システムの共同利用についても合わせて推進が期待されると考えられる。
- 番号制度の導入に当たって求められる情報システムの全体像や要件については、未だ検討段階である。しかしながら、番号制度は更なる自治体クラウド推進の契機と捉えられるため、今後の検討内容も踏まえ、番号制度と自治体クラウドをより一層、一体的に推進していくことが重要と考えられる。